Express Mail Label No.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YO999-097
Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

INTELLIGENT ANTITHEFT METHOD AND SYSTEM COMBINING MAGNETIC TAGS AND SMART CARDS

and invented by:

Alejandro Gabriel Schrott, Michael J. Steinmetz, Robert Jacob von Gutfeld, and James Peter Ward

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having **15** pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☐ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Microfiche Appendix *(if applicable)*
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if drawings filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b)).

Docket No. YO999-097
Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*

   a. ☐ Formal Number of Sheets _____

   b. ☒ Informal Number of Sheets **3 (Figs. 1-4)**

4. ☒ Oath or Declaration

   a. ☒ Newly executed *(original or copy)* ☐ Unexecuted

   b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*

   c. ☒ With Power of Attorney ☐ Without Power of Attorney

   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Computer Program in Microfiche *(Appendix)*

7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*

   a. ☐ Paper Copy

   b. ☐ Computer Readable Copy *(identical to computer copy)*

   c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☒ Assignment Papers *(cover sheet & document(s))*

9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*

10. ☐ English Translation Document *(if applicable)*

11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations

12. ☐ Preliminary Amendment

13. ☒ Acknowledgment postcard

14. ☐ Certificate of Mailing

   ☐ First Class ☐ Express Mail *(Specify Label No.):* _____

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. YO999-097
Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☐ Additional Enclosures *(please identify below):*

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	20	- 20 =	0	x	$18.00	$0.00
Indep. Claims	2	- 3 =	0	x	$78.00	$0.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$760.00
OTHER FEE *(specify purpose)*		**Assignment Recordation**				$40.00
					TOTAL FILING FEE	$800.00

☒ A check in the amount of **$800.00** to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **50-0481** as described below. A duplicate copy of this sheet is enclosed.

- ☐ Charge the amount of as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Sean M. McGinn

Signature

Dated: **May 7, 1999**

Sean M. McGinn, Esq.
Registration No.: 34,386

cc:

Customer No.: 21254

MCGINN & GIBB, P.C.
A PROFESSIONAL LIMITED LIABILITY COMPANY
PATENTS, TRADEMARKS, COPYRIGHTS, AND INTELLECTUAL PROPERTY LAW
1701 CLARENDON BOULEVARD, SUITE 100
ARLINGTON, VIRGINIA 22209
TELEPHONE (703) 294-6699
FACSIMILE (703) 294-6696

APPLICATION FOR UNITED STATES LETTERS PATENT

APPLICANTS: Alejandro Gabriel Schrott, Michael J. Steinmetz, Robert Jacob von Gutfeld, and James Peter Ward

FOR: INTELLIGENT ANTITHEFT METHOD AND SYSTEM COMBINING MAGNETIC TAGS AND SMART CARDS

DOCKET NO.: YO999-097

INTELLIGENT ANTITHEFT METHOD AND SYSTEM COMBINING MAGNETIC TAGS AND SMART CARDS

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to an antitheft method and system, and more particularly to an antitheft method and system employing a magnetic tag on an item and a smart card for disabling a theft detector.

Description of the Related Art

Conventional systems are known which include a mechanism (and technique) for disabling an object (e.g., computer). For example, in a retail establishment, typically a system incorporating a security gate as an interrogation device is used. Typically, retail objects are affixed with a tag (e.g., magnetic tag or the like). If the object has been purchased legitimately, then the magnetic field/radio frequency field in the tag is nullified at the point of purchase. As the customer traverses through the gate, the object incorporating such a tag is interrogated, but since the tag's field has been nullified, there is no alarm.

By the same token, if a shoplifter attempts to traverse through the gate with the tag intact and operable (e.g., not nullified by the clerk or the like), then the gate will interrogate the tag affixed to the object. Since the tag has not been rendered inoperable by a tag reader held by the clerk or the like, the gate will notify an alarm (e.g., audio and/or visual). Typically, the alarm can be turned off only by the store personnel, not by the consumer, even if the consumer legitimately purchased the item.

Thus, this method is extremely inconvenient, especially in the case of a computer in a retail or office environment because the computer may become disabled and, if recovered, must be reenabled. Further, such a method would be very disruptive in an office environment where an alarm would be activated and not be able to be deactivated by a legitimate user/owner of the computer. Additionally, in such a conventional system and method, as described in, for example, U.S. Patent No. 5,874,902, disabling and reenabling of the computer is performed, but is a very cumbersome and time-consuming process.

SUMMARY OF THE INVENTION

In view of the foregoing and other problems of the conventional method and systems, an object of the present invention is to provide a structure and method for incorporating a smart card or the like to disable an anti-theft path (gate) for legitimate purposes.

In a first aspect of the present invention, a system (and method) for preventing theft of an object, includes an electronic article surveillance (EAS) device (e.g., a 1-bit magnetic tag, as made, for example, by Sensormatic Corporation, or a 1-bit radio frequency (RF) tag, as made, for example, by Checkpoint Systems, Inc.), operatively attached to an object, a security path for detection of the EAS device, a reader operatively coupled to the gate, and a smart card for being read by the reader, the smart card containing an identification profile of an authorized user of the object.

Such a method and system allow fast, reliable tracking of personnel carrying objects (computers) into/out of an area. Further, a legitimate user can easily disable an interrogation device upon the presentation of suitable credentials (e.g., a smart card or the like).

Additionally, such a method and system are much more convenient than having the object (e.g., a computer) disabled and then having to reenable the computer upon recovery or if a mistake has occurred. That is, with the invention, the disabling function is part of the interrogation path (e.g., gate). Thus, only the gate need be disabled and then subsequently reenabled, as opposed to the object (e.g., computer) itself. This disabling/reenabling of the gate significantly simplifies the antitheft problem.

Further, the tag on the object (computer) can be a low-cost tag (e.g., a 1-bit tag or the like). Such a low-cost tag reduces the overall cost of implementing the system.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a schematic diagram of a practical system 100 according to a preferred embodiment of the present invention;

Figure 2 illustrates a user traversing a path (e.g., gate 11) of the system and using a smart card 12 or the like according to the present invention;

Figure 3 illustrates an object 20 (e.g., personal computer) including an electronic article surveillance (EAS) device 10 coupled thereto; and

Figure 4 illustrates an internal configuration of a computer 30 of the system 100 according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring now to the drawings, and more particularly to Figures 1-4, a system 100 and associated method for preventing theft of object(s) (e.g., a computer or the like) theft in an office or retail environment, according to the present invention, are shown.

Generally, the present invention prevents opportunity theft of objects such as computers (especially portable computers) that occurs when such objects are left unattended.

As shown in Figures 1 and 3, the system 100 includes an antitheft device 10 such as an electronic article surveillance (EAS) device 10 (e.g., a "tag" or the like) operatively attached to an object 20 (e.g., hereafter for exemplary purposes a computer will be assumed to be "object" 20).

The tag 10 may be any one or more of an acousto-magnetic tag commercially available from Sensormatic Corporation (e.g., commercially available under the tradenames of Ultramax® and Ultrastrip®), a low frequency tag, having a frequency in a range of about 100 to about 1000 Hz and in the form of wires and strips that produce a predetermined, rich harmonic field, and a radio frequency identification (RF) tag in the MHz range (e.g., in a narrow bandwidth at or around 8 MHz or at or around 13 MHz, as prescribed for commercial use by the FCC) similar to that produced by Checkpoint Systems, Inc. as flat resonant 1-bit disposable tags.

Further, the system 100 includes an "intelligent" security gate 11 for detection of the tag 10. Alternatively or additionally to the gate 11, other interrogation devices which could be employed include a manual scanner, or a device referred to as an "EZ Pass" or a "Flash Pass" having, for example, a ceiling-mounted transmitter or the like, and currently being used at toll booths, fuel

stations, etc. for interrogating a tag (card). By simply "flashing" the pass, the interrogating device/alarm could be deactivated.

Additionally, in the vicinity of the gate or integrally built into the gate, preferably a smart card reader 12 is utilized in association with the gate 11. That is, a smart card 21 which contains an identification profile of the user also is utilized.

As shown in Figure 1, the smart card reader 12 preferably is connected to a computer 30 containing a database 301. The computer is shown in further detail in Figure 4. The database 301 includes information regarding the identity of the authorized user of the computer 20. As shown in Figure 4, the database 301 receives an output from the smart card reader regarding the identity profile of the user.

The database 301 through a comparator function or the like compares user identification information from the smart card with information in the database regarding the user.

Along these lines, the computer could be part of a local area network (LAN) or be coupled (via dial-up modem or the like) to an external network such as the World-Wide-Web (WWW) for access to other information and databases.

Upon passage through the gate 11 (e.g., in the direction of Arrow A in Figure 1), the tag 10, operatively attached to the computer 20, triggers the gate 11 to selectively notify an alarm system 40, in the standard way that gates are commonly utilized in the retail industry. The alarm 40 also may be coupled to a central guard station which also contains the video receiver 50.

In an exemplary implementation, the invention preferably briefly (e.g., 5 seconds) turns off the alarm and/or opens a physical gate (allowing free passage of the user), when an authorized person exhibits his/her smart card 21 to the reader 12 located in the proximity of the gate 11. The reader 12 is connected to (or integrally formed with) computer 30 having the database 301 containing information on the personnel authorized to enter or exit the premises carrying the computer 20.

Preferably, a function of the computer 30 includes logging the time and user identity related to the passage to the gate 11. Further, the smart card reader 12 could have information regarding the computer assigned to the user traversing the gate 11.

The smart card 21 and reader 12 include direct contact and contact-less models. It is noted that, e.g., by using some zero-knowledge protocol, a smart card can be authenticated but cannot be duplicated, and one has no access to some of the information stored in the smart card if so desired, while what is stored there can be used during the usage of the smart card, to generate other information. This property is what the present inventors consider to be the characterization of a smart card, for purposes of the present application.

Accordingly, in the present disclosure, any electronic component with these properties and which has some memory and/or some processing capabilities, will be called "a smart component" or "a smart card", even if it does not actually take any form resembling a "card". A general reference to smart card

technology and applications can be found in "Smart Cards: A Guide to Building And Managing Smart Card Applications" by Henry Dreifus and J. Thomas Monk, John Wiley & Sons, 1998.

Moreover, the card need not be "smart" but could contain a magnetic strip capable of containing a code. Further, the information in the smart card etc. could be coupled to the user's biometrics (e.g., physical or acquired characteristics possessed solely by the user).

As shown in Figure 2, a camera 60 formed nearby, adjacent or integrally within the gate 11 visually records the person passing through the gate 11 when the alarm 40 rings. The image formed by the camera 60 can be provided to the above-mentioned video receiver 50 optionally coupled to a display, that may be located in a security office and possibly also on a video tape for later inspection. The video receiver is especially useful for single-bit magnetic tags, since the information carried by such tags is very limited, and thus the video receiver assists in identifying personnel.

Alternatively, a video image is captured every time the alarm 40 is actuated (e.g., sounds or visually alerts), and every time the alarm 40 is shut off. This procedure will yield a record of the number of computers taken legally as well as illegally. The camera record will also prevent tailgating by an unauthorized person when the gate 11 is legitimately shut off by the first person entering the gate 11. Alternatively, proper spacing could be ensured by an "electric eye" (photosensor) for detecting a space occurring after a user has inserted his/her smart card into the

smart card reader 12, a heat sensing mechanism which detects a break in any heat-radiating form carrying an object of interest and having identified itself with a smart card 11. A break detected by the heat sensor would indicate someone tailgating the authorized user.

Thus, with the above-described invention, fast, reliable tracking of personnel carrying objects (computers) into/out of an area is provided. Further, a legitimate user can easily disable an interrogation device upon the presentation of suitable credentials (e.g., a smart card or the like).

While the invention has been described in terms of preferred embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.

CLAIMS

What is claimed is:

1. A system for preventing theft of an object, comprising:

an electronic article surveillance (EAS) device operatively attached to an object;

a security path for detection of said EAS device;

a reader operatively coupled to said security path; and

a smart card for being read by said reader, said smart card containing an identification profile of an authorized user of said object.

2. The system according to claim 1, wherein said EAS device comprises an acousto-magnetic tag.

3. The system according to claim 1, wherein said EAS device comprises a low frequency tag having a frequency in a range of about 100 Hz to about 1000 Hz,

said low frequency tag being formed of a pattern of wires and strips that produce a predetermined harmonic field.

4. The system according to claim 1, wherein said EAS device comprises a radio frequency (RF) tag.

5. The system according to claim 1, wherein said security path includes a gate for interrogating said EAS device, said gate including said reader one of built integrally thereto and in a proximity thereof.

6. The system according to claim 1, further comprising a computer coupled to said reader, said computer containing a database including information regarding said authorized user of said object.

7. The system according to claim 1, further comprising an alarm operatively coupled to said security path,

wherein upon passage through said path, said EAS device triggers the path to activate said alarm.

8. The system according to claim 7, further comprising a video receiver operatively coupled to said path, said path activating said video receiver upon interrogating said EAS device.

9. The system according to claim 7, wherein one of said alarm is turned off and an authorized user is allowed free passage through said path, when said authorized person exhibits said smart card to said reader.

10. The system according to claim 1, further comprising a storage device, coupled to said reader, containing information on personnel authorized to enter through or exit through said path with said object.

11. The system according to claim 6, wherein said computer logs a time and user identity related to passage through said path.

12. The system according to claim 1, wherein said smart card comprises a direct contact smart card.

13. The system according to claim 1, wherein said smart card comprises a contact-less smart card.

14. The system according to claim 1, wherein said smart card comprises a magnetic strip containing a code.

15 A method for preventing theft of an object, comprising:

operatively attaching an electronic article surveillance (EAS) device to an object;

detecting said EAS device as said object traverses a security path;

operatively coupling a reader to said security path; and

reading, by said reader, a smart card being presented to said reader as said object traverses said security path, said smart card containing an identification profile of an authorized user of said object.

16. The method according to claim 15, wherein said EAS device comprises an acousto-magnetic tag.

17. The method according to claim 15, wherein said EAS device comprises a low frequency tag having a frequency in a range of about 100 Hz to about 1000 Hz,

said low frequency tag being formed of a pattern of wires and strips that produce a predetermined harmonic field.

18. The method according to claim 15, wherein said EAS device comprises a radio frequency (RF) tag.

19. The method according to claim 15, wherein said security path includes a gate for interrogating said EAS device, said gate including said reader one of built integrally thereto and in a proximity thereof.

20. The method according to claim 15, further comprising:

coupling a computer to said reader, said computer containing a database including information regarding said authorized user of said object; and

operatively coupling an alarm to said security path,

wherein upon passage through said path, said EAS device triggers the path to activate said alarm.

INTELLIGENT ANITTHEFT METHOD COMBINING MAGNETIC TAGS AND SMART CARDS

ABSTRACT

A method and system for preventing theft of an object, includes an electronic article surveillance (EAS) device operatively attached to an object, a security path for detection of the EAS device, a reader operatively coupled to the security path, and a smart card for being read by the reader. The smart card contains an identification profile of an authorized user of the object.

100

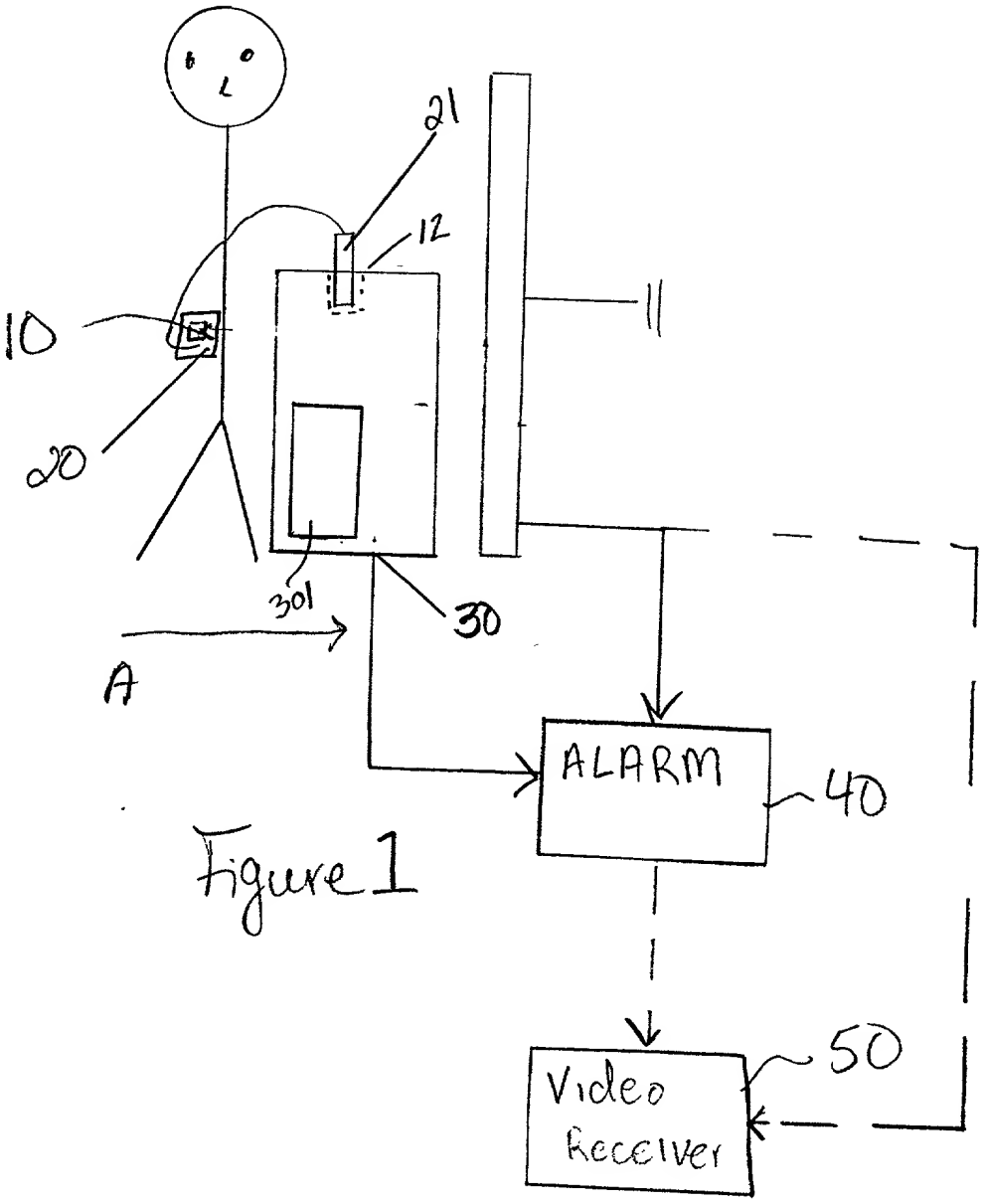

Figure 1

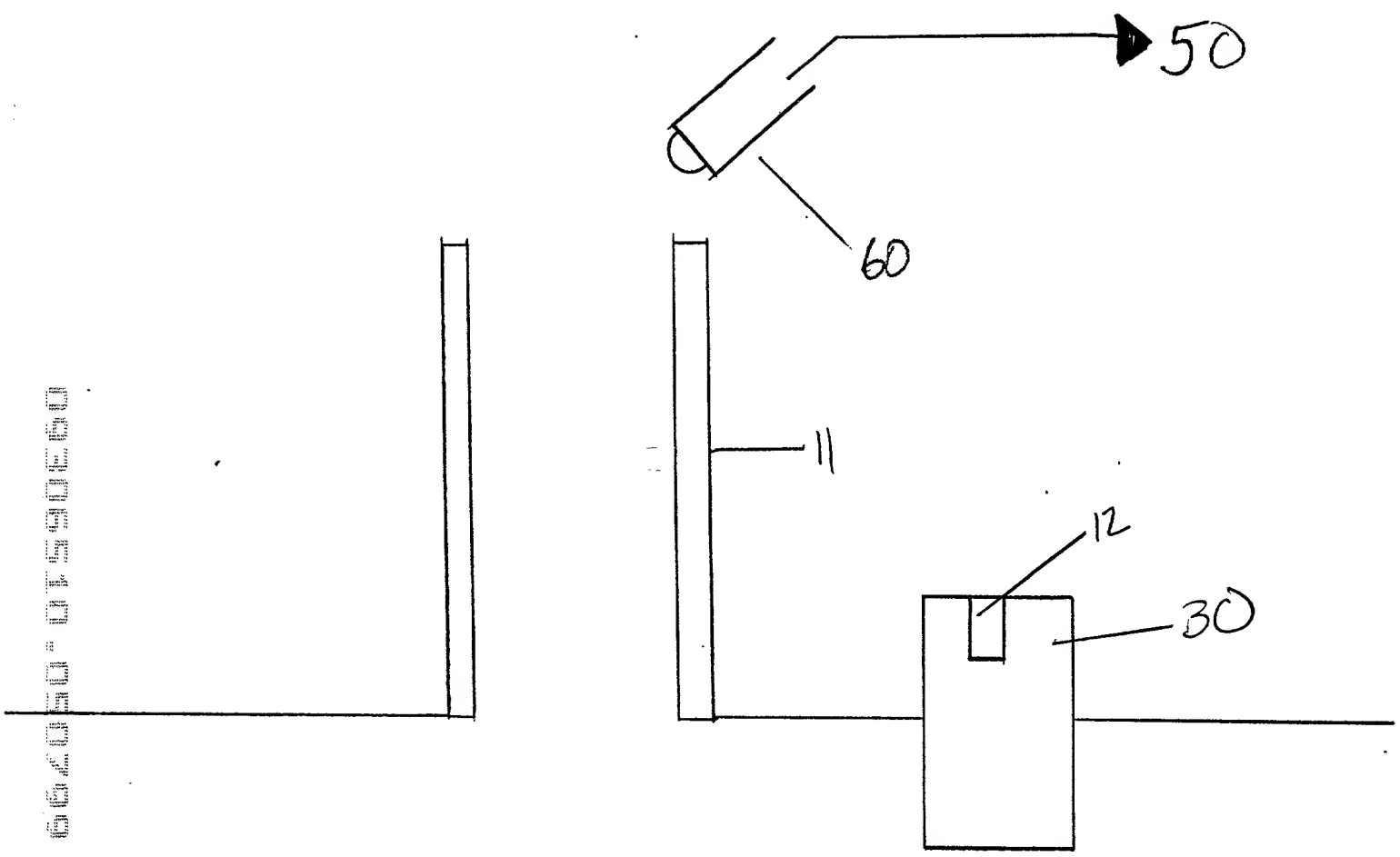

figure 2

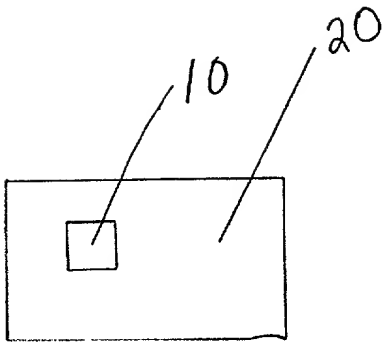

Fig. 3

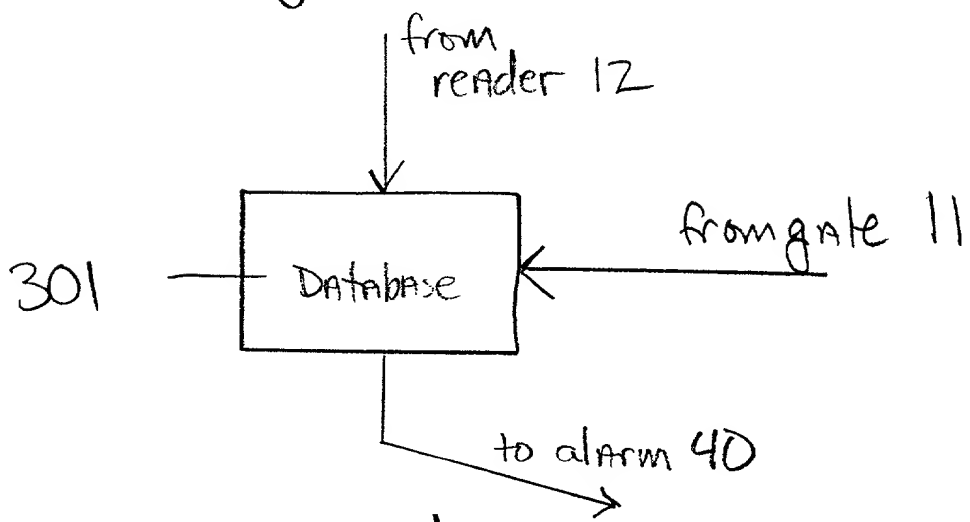

Fig. 4

IBM Docket No.: YO999-097

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: INTELLIGENT ANTITHEFT METHOD AND SYSTEM COMBINING MAGNETIC TAGS AND SMART CARDS

the specification of which:
(check one)

☒ is attached hereto.
☐ was filed on _____, as Application Serial No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

Number	Country	Day/Month/Year	Priority Claimed

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Applications:

Serial No.	Filing Date	Status

I hereby declare that all statements made herein of my own knowledge are true arid that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: We hereby appoint Manny Schecter, Registration No.31,722, Terry J. Ilardi, Registration No. 29,936, Christopher A. Hughes, Registration No. 26,914, Edward A. Pennington, Registration No. 32,588, John E. Hoel, Registration No. 26,279, Joseph C. Redmond, Jr., Registration No. 18,753, Douglas W. Cameron, Registration No. 31,596, Louis P. Herzberg, Registration No. 41,500, Kevin M. Jordan, Registration No.40,277, Stephen C. Kaufman, Registration No.29,551, Daniel P. Morris, Registration No.32,053, Louis J. Percello, Registration No.33,206, Jay P. Sbrollini, Registration No. 36,266, David M. Shofi, Registration No. 39,835, Paul J. Otterstedt, Registration No. 37,411 and Robert M. Trepp, Registration No. 25,933, to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith.

Send all correspondence to: **McGinn & Gibb, P.C., 1701 Clarendon Boulevard, Suite 100, Arlington, Virginia 22209. Customer No. 21254**

Telephone calls should be directed to Sean M. McGinn, McGinn & Gibb, P.C. at (703) 294-6699.

(1) Inventor: Alejandro Gabriel Schrott

Signature: Alejandro Gabriel Schrott Date: 5/3/99

Residence: 175 West 12th Street, Apt. 9-B, New York, New York 10011

Citizenship: United States of America

Post Office Address: Same as Above

(2) Inventor: Michael J. Steinmetz

Signature: Michael J Steinmetz Date: 5/4/1999

Residence: 102 Marsden Court, Cary, NC 27511

Citizenship: United States of America

Post Office Address: Same as Above

(3) Inventor: Robert Jacob von Gutfeld

Signature: Robert Jacob von Gutfeld Date: 5/3/99

Residence: 600 West 115th Street, Apt. 113, New York, New York 10025

Citizenship: United States of America

Post Office Address: Same as Above

(4) Inventor: James Peter Ward

Signature: James Peter Ward Date: 5/4/99

Residence: 107 Hemingway Forest Place, Raleigh, NC 27607

Citizenship: United States of America

Post Office Address: Same as Above